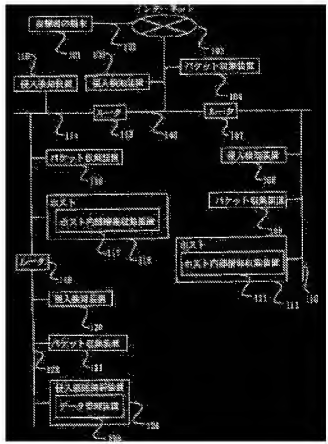
SYSTEM AND METHOD FOR ANALYZING ILLEGAL ACCESS ROUTE

Publication number: JP2003258910 (A)
Publication date: 2003-09-12
Inventor(s): KITAZAWA SHIGEKI +
Applicant(s): MITSUBISHI ELECTRIC CORP +
Classification:
- international: ***G06F13/00; G06F15/00; H04L12/22; H04L12/56;*** **G06F13/00; G06F15/00; H04L12/22; H04L12/56;** (IPC1-7): G06F13/00; G06F15/00; H04L12/22; H04L12/56
- European:
Application number: JP20020056913 20020304
Priority number(s): JP20020056913 20020304

Also published as:
JP3892322 (B2)

Abstract of **JP 2003258910 (A)**

PROBLEM TO BE SOLVED: To realize intrusion route analysis which is applicable to intrusion using a steppingstone and intrusion using a false transmission-source address. SOLUTION: A packet gathering device 104, etc., records the header contents of a packet sent through a network as header information and a host internal information gathering device 111, etc., gathers internal process information regarding internal processes of a host 112, etc. An intrusion route analyzing device 124 receives the header information and internal process information and a data management device 123 manages data as a database; ; when an intrusion packet is detected, the transmission source of the intrusion packet is detected by using host level analysis and router level analysis in combination and when the transmission source of the intrusion packet is a host in the network, a packet which contributes the generation and transmission of the intrusion packet is specified by taking host internal analysis of the host to analyze the intrusion route by using the three analyzing processes in combination. ; COPYRIGHT: (C) 2003,JPO



(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号
特開2003－258910
（P2003－258910A）
(43)公開日　平成15年９月12日(2003.9.12)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード（参考）
Ｈ０４Ｌ　12/56	４００	Ｈ０４Ｌ　12/56	４００Ｚ	５Ｂ０８５
Ｇ０６Ｆ　13/00	３５１	Ｇ０６Ｆ　13/00	３５１Ｚ	５Ｂ０８９
15/00	３２０	15/00	３２０Ａ	５Ｋ０３０
Ｈ０４Ｌ　12/22		Ｈ０４Ｌ　12/22		

審査請求　未請求　請求項の数16　ＯＬ　（全 16 頁）

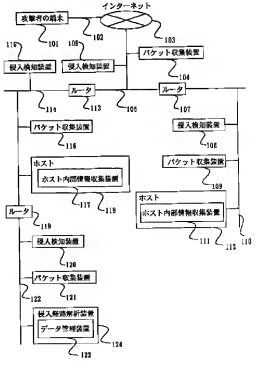
(21)出願番号　特願2002－56913(P2002－56913)
(22)出願日　平成14年３月４日(2002.3.4)

(71)出願人　000006013
三菱電機株式会社
東京都千代田区丸の内二丁目２番３号
(72)発明者　北澤　繁樹
東京都千代田区丸の内二丁目２番３号　三菱電機株式会社内
(74)代理人　100099461
弁理士　溝井　章司　（外５名）

Ｆターム(参考)　5B085 AC11
5B089 GB02 KA17 KB13
5K030 GA15 HA08 JA10 KA05 KX24
KX30 LC14 LC15 LD19

(54)【発明の名称】　不正アクセス経路解析システム及び不正アクセス経路解析方法

(57)【要約】
【課題】　踏み台を用いた侵入、発信元アドレスを詐称した侵入に対しても対応可能な侵入経路解析を実現する。
【解決手段】　パケット収集装置１０４等がネットワーク上を流れるパケットのヘッダ内容をヘッダ情報として記録し、ホスト内部情報収集装置１１１等がホスト１１２等の内部プロセスに関する内部プロセス情報を収集し、侵入経路解析装置１２４はヘッダ情報及び内部プロセス情報を受信するとともにデータ管理装置１２３においてデータベースとして管理し、侵入パケットの検知の際に、ホストレベル解析及びルータレベル解析を併用して侵入パケットの送信元を検出し、侵入パケットの送信元がネットワーク内のホストであった場合には、当該ホストに対してホスト内部解析を行って侵入パケットの生成・送信に関与したパケットを特定し、以後、３つの解析処理を併用して侵入経路の解析を行う。



1

【特許請求の範囲】

【請求項１】　相互にパケット送受信を行い得る複数のデータ処理装置を含む所定のネットワークを管理対象とし、前記ネットワークに含まれるいずれかのデータ処理装置に対して不正アクセスパケットが送信された場合に、不正アクセスパケットの送信に用いられた不正アクセス経路の解析を行う不正アクセス経路解析システムであって、

前記ネットワークを流通するパケットを監視し、不正アクセスパケットを検知するパケット監視部と、

前記パケット監視部により不正アクセスパケットが検知された場合に、不正アクセスパケットの送信元の検出処理を行い、所定の場合に、前記複数のデータ処理装置のうち特定のデータ処理装置を不正アクセスパケットの送信元として検出する送信元検出処理部と、

前記送信元検出処理部により特定のデータ処理装置が不正アクセスパケットの送信元として検出された場合に、前記送信元検出処理部により検出されたデータ処理装置の内部プロセスについて解析処理を行って、不正アクセスパケットの生成及び送信を実行した内部プロセスを不正アクセスパケット生成送信プロセスとして検出するとともに、所定の場合に、前記不正アクセスパケット生成送信プロセスに関連するパケット受信プロセスを検出し、検出した前記パケット受信プロセスにおいて受信されたパケットを不正アクセスパケットとして認定する内部プロセス解析処理部とを有し、

前記送信元検出処理部は、

前記内部プロセス解析処理部により不正アクセスパケットの認定が行われた場合に、認定された不正アクセスパケットの送信元の検出処理を行うことを特徴とする不正アクセス経路解析システム。

【請求項２】　前記不正アクセス経路解析システムは、更に、

前記複数のデータ処理装置の各々の内部プロセスを監視し、所定の場合に、前記内部プロセス解析処理部に特定のデータ処理装置に関する通知を行う内部プロセス監視部を有し、

前記内部プロセス解析処理部は、

前記内部プロセス監視部から通知されたデータ処理装置の内部プロセスについて解析処理を行い、不正アクセスパケット生成送信プロセスに関連するパケット受信プロセスが検出された場合に、不正アクセスパケットの認定を行い、

前記送信元検出処理部は、

前記内部プロセス解析処理部により不正アクセスパケットの認定が行われた場合に、認定された不正アクセスパケットの送信元の検出処理を行うことを特徴とする請求項１に記載の不正アクセス経路解析システム。

【請求項３】　前記送信元検出処理部及び前記内部プロセス解析処理部は、相互に連動してそれぞれの処理を行い、

2

前記送信元検出処理部は、

前記内部プロセス解析処理部により不正アクセスパケットの認定が行われる度に、認定された不正アクセスパケットの送信元の検出処理を行い、所定の場合に、特定のデータ処理装置を不正アクセスパケットの送信元として検出し、

前記内部プロセス解析処理部は、

前記送信元検出処理部により特定のデータ処理装置が不正アクセスパケットの送信元として検出される度に、前記送信元検出処理部により検出されたデータ処理装置の内部プロセスについて解析処理を行い、不正アクセスパケット生成送信プロセスに関連するパケット受信プロセスが検出された場合に、不正アクセスパケットの認定を行うことを特徴とする請求項１又は２に記載の不正アクセス経路解析システム。

【請求項４】　前記内部プロセス解析処理部は、

特定のデータ処理装置の内部プロセスについて解析処理を行った結果、不正アクセスパケット生成送信プロセスに関連するパケット受信プロセスが検出されなかった場合に、前記特定のデータ処理装置を不正アクセスの始点と判断することを特徴とする請求項１～３のいずれかに記載の不正アクセス経路解析システム。

【請求項５】　前記不正アクセス経路解析システムは、データ処理装置間に少なくなくとも一つ以上のパケット中継装置が配置されたネットワークを管理対象とし、

前記送信元検出処理部は、

不正アクセスパケットを受信したデータ処理装置を始点として、不正アクセスパケットを中継したパケット中継装置を論理的に順次遡って不正アクセスパケットの送信元を検出する第一の送信元検出処理と、

不正アクセスパケットに含まれた送信元を示す送信元アドレス情報に基づき、不正アクセスパケットの送信元を検出する第二の送信元検出処理とを並行して行うことを特徴とする請求項１～３のいずれかに記載の不正アクセス経路解析システム。

【請求項６】　前記第二の送信元検出処理は前記第一の送信元検出処理よりも早期に完了する場合があり、

前記内部プロセス解析処理部は、

前記第二の送信元検出処理が前記第一の送信元検出処理よりも早期に完了し、不正アクセスパケットの送信元として特定のデータ処理装置が検出された場合に、前記第二の送信元検出処理により検出されたデータ処理装置の内部プロセスについて解析処理を行い、

前記第二の送信元検出処理により検出されたデータ処理装置の内部プロセスについての解析処理の実行中に、前記第一の送信元検出処理が完了し前記第二の送信元検出処理とは異なるデータ処理装置が不正アクセスパケットの送信元として検出された場合に、前記第二の送信元検出処理により検出されたデータ処理装置の内部プロセス

についての解析処理を終了し、前記第一の送信元検出処理により検出されたデータ処理装置の内部プロセスについての解析処理を開始することを特徴とする請求項５に記載の不正アクセス経路解析システム。

【請求項７】　前記不正アクセス経路解析システムは、更に、

前記ネットワーク内の少なくとも一以上の箇所で前記ネットワークを流通する複数のパケットを収集し、収集した複数のパケットのヘッダの内容を複数のヘッダ情報として記録し、記録した複数のヘッダ情報を前記送信元検出処理部に送信するパケット収集部を有し、

前記送信元検出処理部は、

前記パケット収集部より前記複数のヘッダ情報を受信するとともに、

前記第一の送信元検出処理として、

データ処理装置が受信した不正アクセスパケットのヘッダに含まれる情報であって送信元ＥｔｈｅｒアドレスＭ、宛先ＥｔｈｅｒアドレスＭ及びＴＴＬ（ＴｉｍｅＴｏ　Ｌｉｖｅ）値以外の情報に基づき、前記複数のヘッダ情報の中から少なくとも一つ以上のヘッダ情報を抽出ヘッダ情報として抽出し、不正アクセスパケットに含まれる送信元ＥｔｈｅｒアドレスＭ、宛先ＥｔｈｅｒアドレスＭ及びＴＴＬ値を始点として抽出ヘッダ情報に含まれる送信元ＥｔｈｅｒアドレスＭ、宛先ＥｔｈｅｒアドレスＭ及びＴＴＬ値の更新経過を順次遡って不正アクセスパケットの送信元を検出することを特徴とする請求項５に記載の不正アクセス経路解析システム。

【請求項８】　前記送信元検出処理部は、

前記第二の送信元検出処理として、

不正アクセスパケットに含まれた送信元ＩＰアドレスに基づき、不正アクセスパケットの送信元を検出することを特徴とする請求項５に記載の不正アクセス経路解析システム。

【請求項９】　前記パケット収集部は、

前記送信元検出処理部から指示があった場合のみ、パケットの収集を行うことを特徴とする請求項７に記載の不正アクセス経路解析システム。

【請求項１０】　前記パケット収集部は、

前記送信元検出処理部から指示があった場合のみ、前記送信元検出処理部に対して前記複数のヘッダ情報を送信することを特徴とする請求項７に記載の不正アクセス経路解析システム。

【請求項１１】　前記不正アクセス経路解析システムは、更に、

前記複数のデータ処理装置の各々について内部プロセスに関する情報を内部プロセス情報として収集し、収集した内部プロセス情報を前記内部プロセス解析処理部へ送信する内部プロセス情報収集部を有し、

前記内部プロセス解析処理部は、

前記内部プロセス情報収集部より前記内部プロセス情報を受信するとともに、受信した内部プロセス情報の中から内部プロセス解析処理の対象となるデータ処理装置の内部プロセス情報を選択し、選択した内部プロセス情報を用いて内部プロセス解析処理を行うことを特徴とする請求項１～３のいずれかに記載の不正アクセス経路解析システム。

【請求項１２】　前記内部プロセス情報収集部は、

前記内部プロセス解析処理部から指示があった場合のみ、内部プロセス情報の収集を行うことを特徴とする請求項１１に記載の不正アクセス経路解析システム。

【請求項１３】　前記内部プロセス情報収集部は、

前記内部プロセス解析処理部から指示があった場合のみ、前記内部プロセス解析処理部に対して前記内部プロセス情報を送信することを特徴とする請求項１１に記載の不正アクセス経路解析システム。

【請求項１４】　前記不正アクセス経路解析システムは、他のネットワークを管理対象とする他の不正アクセス経路解析システムと通信可能であり、

前記他の不正アクセス経路解析システムより、前記他のネットワーク内で検出された他ネットワーク不正アクセスパケットの情報を含む検出依頼を受信した場合に、

前記送信元検出処理部は、

前記検出依頼に含まれた前記他ネットワーク不正アクセスパケットの情報に基づき、前記他ネットワーク不正アクセスパケットの送信元の検出処理を行うことを特徴とする請求項１に記載の不正アクセス経路解析システム。

【請求項１５】　前記不正アクセス経路解析システムは、他のネットワークを管理対象とする他の不正アクセス経路解析システムと通信可能であり、

前記送信元検出処理部が特定の不正アクセスパケットについて送信元が検出できなかった場合に、前記他の不正アクセス経路解析システムに対して前記特定の不正アクセスパケットの送信元の検出を依頼する検出依頼を送信することを特徴とする請求項１に記載の不正アクセス経路解析システム。

【請求項１６】　相互にパケット送受信を行い得る複数のデータ処理装置を含む所定のネットワークを管理対象とし、前記ネットワークに含まれるいずれかのデータ処理装置に対して不正アクセスパケットが送信された場合に、不正アクセスパケットの送信に用いられた不正アクセス経路の解析を行う不正アクセス経路解析方法であって、

前記ネットワークを流通するパケットを監視し、不正アクセスパケットを検知するパケット監視ステップと、

前記パケット監視ステップにより不正アクセスパケットが検知された場合に、不正アクセスパケットの送信元の検出処理を行い、所定の場合に、前記複数のデータ処理装置のうち特定のデータ処理装置を不正アクセスパケットの送信元として検出する送信元検出処理ステップと、

前記送信元検出処理ステップにより特定のデータ処理装

置が不正アクセスパケットの送信元として検出された場合に、前記送信元検出処理ステップにより検出されたデータ処理装置の内部プロセスについて解析処理を行って、不正アクセスパケットの生成及び送信を実行した内部プロセスを不正アクセスパケット生成送信プロセスとして検出するとともに、所定の場合に、前記不正アクセスパケット生成送信プロセスに関連するパケット受信プロセスを検出し、検出した前記パケット受信プロセスにおいて受信されたパケットを不正アクセスパケットとして認定する内部プロセス解析処理ステップとを有し、

前記送信元検出処理ステップは、

前記内部プロセス解析処理ステップにより不正アクセスパケットの認定が行われた場合に、認定された不正アクセスパケットの送信元の検出処理を行うことを特徴とする不正アクセス経路解析方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明は、侵入経路解析システム並びに、侵入経路解析手法の高速化に関するものである。

【０００２】

【従来の技術】図２は例えば、特開２０００－３４１３１５および特開２０００－１２４９５２に示されたパケットの情報を解析する従来の侵入経路解析システムを示す。図２において、２０１は攻撃者端末、２０２はインターネット、２０３は攻撃者端末が直接接続しているアクセスサーバ、２０６は踏み台ホスト、２１１は不正アクセス対象ホスト、２１０は侵入検知装置、２０４、２０５は攻撃者端末２０１から踏み台ホスト２０６へのパケットを中継した追跡装置（ルータ）、２０７、２０８、２０９は踏み台ホストから不正アクセス対象ホストへのパケットを中継した追跡装置（ルータ）である。攻撃者は、踏み台ホスト２０６を使用することで不正アクセス対象ホスト２１１に対して攻撃者端末の身元を隠蔽して不正アクセスを行っているものとする。

【０００３】このような従来の侵入追跡システムにおいては、不正アクセス対象ホスト２１１から踏み台ホスト２０６までの追跡と踏み台ホスト２０６から攻撃者端末２０１までの追跡処理が複数の段階を経る。どの段階においても不正アクセスパケットの情報を元に追跡管理装置２１２が追跡経路上に存在する複数の追跡装置（ルータ）へ追跡を指示し、その結果からさらにその先の追跡装置（ルータ）へ追跡を指示するといった逐次的な追跡を継続することで攻撃者端末２０１が直接接続しているアクセスサーバ２０３まで追跡を行う。最終的な攻撃者端末２０１の特定はアクセスサーバ２０３の接続ログを解析することで行う。

【０００４】図３は例えば、特開平１０－１６４０６４に示された接続経路情報をホスト間の接続ごと、あらかじめ記録として残しておく従来の侵入経路解析システムである。図３において、３０１はネットワーク管理マネージャ、３０２、３０３、３０４は計算機ノード、３０５は追跡情報収集操作、３０６はセキュリティ上の問題通知を表している。図において、計算機ノード３０２から計算機ノード３０３を踏み台として、計算機ノード３０４へ不正なアクセスを行っているものとする。また、各計算機ノードは、リモートから接続が行われたとき、その接続の経路追跡を行うための情報をあらかじめ記録しておく。

【０００５】このような従来の侵入追跡システムにおいては、図３の計算機ノード３０３から計算機ノード３０４へ接続を要求した場合、計算機ノード３０４は、経路追跡に使用する接続経路情報を計算機ノード３０３へ要求する。計算機ノード３０３は、接続を要求している計算機ノード３０３上のプロセスの識別子と計算機ノード３０３の識別子を計算機ノード３０４へ送る。同様の手続きは、計算機ノード間の接続が発生するたびに行われているものとする。セキュリティ上の問題が計算機ノード３０４上で起こったとき、ネットワーク管理マネージャ３０１は計算機ノード３０４からのセキュリティ上の問題通知３０６を受け取り、計算機ノード３０４上に記録されている、そのセキュリティ上の問題を発生させる元となった接続経路情報を元に、計算機ノード３０３へ計算機ノード３０４との接続経路情報を問い合わせる。計算機ノード３０３では、計算機ノード３０４への接続は計算機ノード３０２からの接続により起動されたプロセスによより発生していることをネットワーク管理マネージャ３０１へ通知する。次にネットワーク管理マネージャ３０１は、計算機ノード３０２へ接続経路情報の問い合わせを行い、最終的に計算機ノード３０２が不正なアクセスを行った接続経路の発信源であると特定する。

【０００６】

【発明が解決しようとする課題】従来の侵入経路解析システムのうち、特開２０００－３４１３１５及び特開２０００－１２４９５２に示されたものは、パケットのヘッダ情報を元に侵入経路を解析することでＩＰパケットのヘッダ情報に含まれている発信元アドレスを詐称した不正アクセスパケットの追跡が可能という利点がある反面、踏み台を介した攻撃については、踏み台ホストの入出力を監視し、不正アクセスパケットが再び踏み台ホストへ送信されるのを待つ必要があり、侵入経路追跡の継続性を積極的に維持できない、追跡時間がかかるなどの問題点があった。一方、接続経路情報をホスト間の接続ごとにあらかじめ記録として残しておく方式（特開平１０－１６４０６４）では、侵入経路追跡にかかる時間を短縮できる代わりに、ＩＰパケットのヘッダ情報に含まれている発信元アドレスを詐称した攻撃では、偽の接続経路情報が記録されることもありうるため、正確性に問題点があった。また、いずれの場合にも追跡処理を管理するホストが侵入経路上のルータもしくは、接続ホスト

一つ一つと通信を行いながら逐次追跡していくため、侵入経路上のルータおよびホストの数に比例して侵入経路解析時間が増加する問題点があった。

【０００７】この発明は上記のような問題点を解決するためになされたもので、攻撃者が身元を隠蔽する行為（例えば発信元ＩＰアドレスの詐称、踏み台ホストの使用など）を行った場合であっても侵入経路解析結果を正確かつ高速に求めることができる侵入経路解析システムのためのシステム構成と解析アルゴリズムに関するものである。

【０００８】

【課題を解決するための手段】本発明に係る不正アクセス経路解析システムは、相互にパケット送受信を行い得る複数のデータ処理装置を含む所定のネットワークを管理対象とし、前記ネットワークに含まれるいずれかのデータ処理装置に対して不正アクセスパケットが送信された場合に、不正アクセスパケットの送信に用いられた不正アクセス経路の解析を行う不正アクセス経路解析システムであって、前記ネットワークを流通するパケットを監視し、不正アクセスパケットを検知するパケット監視部と、前記パケット監視部により不正アクセスパケットが検知された場合に、不正アクセスパケットの送信元の検出処理を行い、所定の場合に、前記複数のデータ処理装置のうち特定のデータ処理装置を不正アクセスパケットの送信元として検出する送信元検出処理部と、前記送信元検出処理部により特定のデータ処理装置が不正アクセスパケットの送信元として検出された場合に、前記送信元検出処理部により検出されたデータ処理装置の内部プロセスについて解析処理を行って、不正アクセスパケットの生成及び送信を実行した内部プロセスを不正アクセスパケット生成送信プロセスとして検出するとともに、所定の場合に、前記不正アクセスパケット生成送信プロセスに関連するパケット受信プロセスを検出し、検出した前記パケット受信プロセスにおいて受信されたパケットを不正アクセスパケットとして認定する内部プロセス解析処理部とを有し、前記送信元検出処理部は、前記内部プロセス解析処理部により不正アクセスパケットの認定が行われた場合に、認定された不正アクセスパケットの送信元の検出処理を行うことを特徴とする。

【０００９】前記不正アクセス経路解析システムは、更に、前記複数のデータ処理装置の各々の内部プロセスを監視し、所定の場合に、前記内部プロセス解析処理部に特定のデータ処理装置に関する通知を行う内部プロセス監視部を有し、前記内部プロセス解析処理部は、前記内部プロセス監視部から通知されたデータ処理装置の内部プロセスについて解析処理を行い、不正アクセスパケット生成送信プロセスに関連するパケット受信プロセスが検出された場合に、不正アクセスパケットの認定を行い、前記送信元検出処理部は、前記内部プロセス解析処理部により不正アクセスパケットの認定が行われた場合に、認定された不正アクセスパケットの送信元の検出処理を行うことを特徴とする。

【００１０】前記送信元検出処理部及び前記内部プロセス解析処理部は、相互に連動してそれぞれの処理を行い、前記送信元検出処理部は、前記内部プロセス解析処理部により不正アクセスパケットの認定が行われる度に、認定された不正アクセスパケットの送信元の検出処理を行い、所定の場合に、特定のデータ処理装置を不正アクセスパケットの送信元として検出し、前記内部プロセス解析処理部は、前記送信元検出処理部により特定のデータ処理装置が不正アクセスパケットの送信元として検出される度に、前記送信元検出処理部により検出されたデータ処理装置の内部プロセスについて解析処理を行い、不正アクセスパケット生成送信プロセスに関連するパケット受信プロセスが検出された場合に、不正アクセスパケットの認定を行うことを特徴とする。

【００１１】前記内部プロセス解析処理部は、特定のデータ処理装置の内部プロセスについて解析処理を行った結果、不正アクセスパケット生成送信プロセスに関連するパケット受信プロセスが検出されなかった場合に、前記特定のデータ処理装置を不正アクセスの始点と判断することを特徴とする。

【００１２】前記不正アクセス経路解析システムは、データ処理装置間に少なくなくとも一つ以上のパケット中継装置が配置されたネットワークを管理対象とし、前記送信元検出処理部は、不正アクセスパケットを受信したデータ処理装置を始点として、不正アクセスパケットを中継したパケット中継装置を論理的に順次遡って不正アクセスパケットの送信元を検出する第一の送信元検出処理と、不正アクセスパケットに含まれた送信元を示す送信元アドレス情報に基づき、不正アクセスパケットの送信元を検出する第二の送信元検出処理とを並行して行うことを特徴とする。

【００１３】前記第二の送信元検出処理は前記第一の送信元検出処理よりも早期に完了する場合があり、前記内部プロセス解析処理部は、前記第二の送信元検出処理が前記第一の送信元検出処理よりも早期に完了し、不正アクセスパケットの送信元として特定のデータ処理装置が検出された場合に、前記第二の送信元検出処理により検出されたデータ処理装置の内部プロセスについて解析処理を行い、前記第二の送信元検出処理により検出されたデータ処理装置の内部プロセスについての解析処理の実行中に、前記第一の送信元検出処理が完了し前記第二の送信元検出処理とは異なるデータ処理装置が不正アクセスパケットの送信元として検出された場合に、前記第二の送信元検出処理により検出されたデータ処理装置の内部プロセスについての解析処理を終了し、前記第一の送信元検出処理により検出されたデータ処理装置の内部プロセスについての解析処理を開始することを特徴とする。

【００１４】前記不正アクセス経路解析システムは、更に、前記ネットワーク内の少なくとも一以上の箇所で前記ネットワークを流通する複数のパケットを収集し、収集した複数のパケットのヘッダの内容を複数のヘッダ情報として記録し、記録した複数のヘッダ情報を前記送信元検出処理部に送信するパケット収集部を有し、前記送信元検出処理部は、前記パケット収集部より前記複数のヘッダ情報を受信するとともに、前記第一の送信元検出処理として、データ処理装置が受信した不正アクセスパケットのヘッダに含まれる情報であって送信元ＥｔｈｅｒアドレスⅠ、宛先ＥｔｈｅｒアドレスⅠ及びＴＴＬ（ＴｉｍｅＴｏ　Ｌｉｖｅ）値以外の情報に基づき、前記複数のヘッダ情報の中から少なくとも一つ以上のヘッダ情報を抽出ヘッダ情報として抽出し、不正アクセスパケットに含まれる送信元ＥｔｈｅｒアドレスⅠ、宛先ＥｔｈｅｒアドレスⅠ及びＴＴＬ値を始点として抽出ヘッダ情報に含まれる送信元ＥｔｈｅｒアドレスⅠ、宛先ＥｔｈｅｒアドレスⅠ及びＴＴＬ値の更新経過を順次遡って不正アクセスパケットの送信元を検出することを特徴とする。

【００１５】前記送信元検出処理部は、前記第二の送信元検出処理として、不正アクセスパケットに含まれた送信元ＩＰアドレスⅠに基づき、不正アクセスパケットの送信元を検出することを特徴とする。

【００１６】前記パケット収集部は、前記送信元検出処理部から指示があった場合のみ、パケットの収集を行うことを特徴とする。

【００１７】前記パケット収集部は、前記送信元検出処理部から指示があった場合のみ、前記送信元検出処理部に対して前記複数のヘッダ情報を送信することを特徴とする。

【００１８】前記不正アクセス経路解析システムは、更に、前記複数のデータ処理装置の各々について内部プロセスに関する情報を内部プロセス情報として収集し、収集した内部プロセス情報を前記内部プロセス解析処理部へ送信する内部プロセス情報収集部を有し、前記内部プロセス解析処理部は、前記内部プロセス情報収集部より前記内部プロセス情報を受信するとともに、受信した内部プロセス情報の中から内部プロセス解析処理の対象となるデータ処理装置の内部プロセス情報を選択し、選択した内部プロセス情報を用いて内部プロセス解析処理を行うことを特徴とする。

【００１９】前記内部プロセス情報収集部は、前記内部プロセス解析処理部から指示があった場合のみ、内部プロセス情報の収集を行うことを特徴とする。

【００２０】前記内部プロセス情報収集部は、前記内部プロセス解析処理部から指示があった場合のみ、前記内部プロセス解析処理部に対して前記内部プロセス情報を送信することを特徴とする。

【００２１】前記不正アクセス経路解析システムは、他のネットワークを管理対象とする他の不正アクセス経路解析システムと通信可能であり、前記他の不正アクセス経路解析システムより、前記他のネットワーク内で検出された他ネットワーク不正アクセスパケットの情報を含む検出依頼を受信した場合に、前記送信元検出処理部は、前記検出依頼に含まれた前記他ネットワーク不正アクセスパケットの情報に基づき、前記他ネットワーク不正アクセスパケットの送信元の検出処理を行うことを特徴とする。

【００２２】前記不正アクセス経路解析システムは、他のネットワークを管理対象とする他の不正アクセス経路解析システムと通信可能であり、前記送信元検出処理部が特定の不正アクセスパケットについて送信元が検出できなかった場合に、前記他の不正アクセス経路解析システムに対して前記特定の不正アクセスパケットの送信元の検出を依頼する検出依頼を送信することを特徴とする。

【００２３】本発明に係る不正アクセス経路解析方法は、相互にパケット送受信を行い得る複数のデータ処理装置を含む所定のネットワークを管理対象とし、前記ネットワークに含まれるいずれかのデータ処理装置に対して不正アクセスパケットが送信された場合に、不正アクセスパケットの送信に用いられた不正アクセス経路の解析を行う不正アクセス経路解析方法であって、前記ネットワークを流通するパケットを監視し、不正アクセスパケットを検知するパケット監視ステップと、前記パケット監視ステップにより不正アクセスパケットが検知された場合に、不正アクセスパケットの送信元の検出処理を行い、所定の場合に、前記複数のデータ処理装置のうち特定のデータ処理装置を不正アクセスパケットの送信元として検出する送信元検出処理ステップと、前記送信元検出処理ステップにより特定のデータ処理装置が不正アクセスパケットの送信元として検出された場合に、前記送信元検出処理ステップにより検出されたデータ処理装置の内部プロセスについて解析処理を行って、不正アクセスパケットの生成及び送信を実行した内部プロセスを不正アクセスパケット生成送信プロセスとして検出するとともに、所定の場合に、前記不正アクセスパケット生成送信プロセスに関連するパケット受信プロセスを検出し、検出した前記パケット受信プロセスにおいて受信されたパケットを不正アクセスパケットとして認定する内部プロセス解析処理ステップとを有し、前記送信元検出処理ステップは、前記内部プロセス解析処理ステップにより不正アクセスパケットの認定が行われた場合に、認定された不正アクセスパケットの送信元の検出処理を行うことを特徴とする。

【００２４】

【発明の実施の形態】実施の形態１．図１は侵入経路解析システム（不正アクセス経路解析システム）の全体図を表す構成図である。ただし、図１はこの侵入経路解析システムの最小単位を示しており、図９のようにそれぞ

れが連携することにより、さらに大きなシステムを構成できる（実施の形態５）。図において、１０１は攻撃者の端末、１０２は攻撃者がインターネットへ接続している経路、１０３はインターネット、１０７、１１３、１１９はルータ、１０５、１０８、１１５、１２０は侵入検知装置、１１２、１１８はホスト、１１１、１１７はホスト内部情報収集装置、１０４、１０９、１１６、１２１はパケット収集装置、１０６、１１０、１１４、１２２はサブネットワーク、１２３はデータ管理装置、１２４は侵入経路解析装置である。ここで、サブネットワークはホスト（複数可）とその他の接続端末によって形成されるローカルネットワークを表す。サブネットワーク（複数可）は、ルータによって相互接続している。図１では、作図の便宜上、ルータ、ホストなどの総数を制限して図示しているが、実運用する場合の総数を制限するものではない。また、図の各装置の配置も実運用の形態を制限するものではないが、１サブネットワーク当り、最低１つのパケット収集装置を配置する。さらに、ホストが存在するサブネットワークには、最低１つの侵入検知装置が存在し、各ホストにホスト内部情報収集装置が存在するものとする。図１に示す侵入検知装置１０５、１０８、１１５、１２０、ホスト内部情報収集装置１１１、１１７、パケット収集装置１０４、１０９、１１６、１２１、侵入経路解析装置１２４により構成されるシステムは、本発明に係る不正アクセス経路解析システムの一例に相当する。

【００２５】図１において、侵入検知装置１０５、１０８、１１５、１２０は、それぞれに割当てられたサブネットワーク上を流れるパケットを監視し、所定の場合に、侵入パケット（不正アクセスパケット又は攻撃パケットともいう）を検知する。侵入検知装置は、パケット監視部に相当する。なお、図１には示していないが、ホスト１１２、１１８の内部プロセス実行状態を監視し、内部プロセスに異常があった場合に侵入があったと判断する侵入検知装置を設けてもよい。このような内部プロセスを監視して侵入を検知する侵入検知装置は、内部プロセス監視部に相当する。ホスト内部情報収集装置１１１、１１７は、それぞれが対象とするホストの内部プロセスに関するホスト内部情報を収集し、収集したホスト内部情報を侵入経路解析装置１２４へ送信する。ホスト内部情報収集装置は、内部プロセス情報収集部に相当する。パケット収集装置１０４、１０９、１１６、１２１は、それぞれが接続されているサブネットワーク上を流れるパケットを捕捉し、捕捉したパケットのヘッダの内容を記録する。記録したヘッダの内容をヘッダ情報と呼ぶ。パケット収集装置は、パケット収集部に相当する。侵入経路解析装置１２４は、パケット収集装置よりヘッダ情報を、ホスト内部情報収集装置よりホスト内部情報を、それぞれ受信し、ヘッダ情報に基づきルータレベル解析及びホストレベル解析を行い、ホスト内部情報に基づきホスト内部解析を行う。侵入経路解析装置１２４は、送信元検出処理部と内部プロセス解析処理部に相当する。なお、ルータレベル解析、ホストレベル解析、ホスト内部解析の詳細については後述する。また、ホスト１１２、１１８は、データ処理装置に、ルータ１０７、１１３、１１９はパケット中継装置に相当する。

【００２６】次に動作について説明する。まず、侵入経路解析装置１２４で侵入経路解析を行うための準備段階としてパケット収集装置並びに、ホスト内部情報収集装置による情報収集を行う。パケット収集装置１０４、１０９、１１６、１２１はそれぞれが接続されているサブネットワーク１０６、１１０、１１４、１２２を流れるパケットを捕捉し、ヘッダの内容をヘッダ情報として記憶領域に記録する。記録するパケットの情報は、パケット取得日時並びに、パケットを識別するために一般的に用いられるパケットヘッダ内の発信元Ｅｔｈｅｒアドレス、宛先ＥｔｈｅｒアドレスIＣＭＰプロトコルヘッダのＴｙｐｅ、Ｃｏｄｅ、Ｃｈｅｃｋｓｕｍ、ＩＰプロトコルヘッダのＩｄｅｎｔｉｆｉｃａｔｉｏｎ、ＴＴＬ（Ｔｉｍｅ Ｔｏ Ｌｉｖｅ）、Ｐｒｏｔｏｃｏｌ、発信元ＩＰアドレス、宛先ＩＰアドレス、ＴＣＰ／ＵＤＰプロトコルヘッダの発信元ポート番号、宛先ポート番号、Ｃｈｅｃｋｓｕｍ、ＴＣＰプロトコルヘッダのＳｅｑｕｅｎｃｅＮｕｍｂｅｒ、ＡｃｋｎｏｗｌｅｄｇｍｅｎｔＮｕｍｂｅｒなどの情報を含む。ホスト内部情報収集装置はホスト上のプロセス管理情報として、プロセス生成日時、プロセス終了日時、プロセス識別子、親プロセス識別子、実ユーザ識別子、実行ユーザ識別子、実グループ識別子、実行グループ識別子、実行ディレクトリ、実行コマンドパス、実行コマンドライン、通信開始日時、通信終了日時、通信先ＩＰアドレス、通信先ＴＣＰ／ＵＤＰポート番号、通信ＮＩＣに割り当てられていたＥｔｈｅｒアドレスとＩＰアドレス、ＴＣＰ／ＵＤＰポート番号などの情報を収集する。収集、記録したこれらの情報は定期的にデータ管理装置１２３へ送信される。データ管理装置１２３は受信したデータを各項目ごとに関連付けてデータベースへ記録する。

【００２７】侵入経路解析装置１２４は、各サブネットワーク上を流れるパケットを監視している侵入検知装置１０５、１０８、１１５、１２０からの侵入検知報告が発生した場合に、自動または手動によって侵入経路解析を開始する。ただし、侵入経路解析を開始する時点において、侵入検知時刻以前にパケット収集装置１０４、１０９、１１６、１２１並びに、ホスト内部情報収集装置１１１、１１７によって収集されたデータは、定期的にデータ管理装置１２３へ送信され、既にデータベースに格納済みであるものとする。

【００２８】ここでは、図１並びに、図４を参照しながら、侵入経路解析装置１２４で行われる侵入経路解析スケジューリングについて説明する。図４は、侵入経路解

析スケジューリングをそれぞれの解析時系列（４１４、４１５、４１６）上に表したものである。図４において、解析時系列（４１４、４１５、４１６）上の長方形は、その解析が実行中であることを示している。図４において、４１４はホストレベル解析を、４１５はホスト内部解析を、４１６はルータレベル解析を示している。

【００２９】ホストレベル解析は、侵入検知装置により検知された侵入パケットに含まれた送信元ＩＰアドレスに基づき、侵入パケットの送信元を検出する解析手法である。また、パケットがたとえばＲＦＣ（Ｒｅｑｕｅｓｔ　ｆｏｒ　Ｃｏｍｍｅｎｔｓ）で規定されるような通信プロトコルに違反していないかどうかの解析も行う。また、パケットのヘッダ情報に含まれる発信元ＩＰアドレスが実際にネットワークへ接続可能なＩＰアドレスであるかどうかなどの調査（ＤＮＳの参照やパケット到達性の検査）もあわせて行う。したがって、一般的には短時間で解析処理が終了する反面、ＩＰアドレスを詐称された場合に対応できないため、解析結果の正確性に乏しい。なお、ホストレベル解析は、第二の送信元検出処理に相当する。一方、ルータレベル解析は、パケット収集装置より送信されたヘッダ情報のうち送信元Ｅｔｈｅｒアドレス、宛先Ｅｔｈｅｒアドレス、ＴＴＬに基づいて、侵入パケットを中継したルータを論理的に順次遡って侵入パケットの送信元を検出する解析手法である。ルータレベル解析は、パケットのＩＰアドレスによらず解析を行うので、ＩＰアドレスを詐称された場合でも正確にパケットの送出ホストと中継経路を特定できる反面、一般的には解析に時間がかかる。なお、ルータレベル解析の具体的手順については後述する。また、ルータレベル解析は、第一の送信元検出処理に相当する。ホスト内部解析は、ホストレベル解析、ルータレベル解析によりホストが特定された場合、またはホスト内部を監視する侵入検知装置によりホストが特定された場合に、特定されたホストの内部プロセス状況を解析し、そのホストが侵入パケットの生成及び送信を行ったか否かを判断するとともに、そのホストが受信したパケットのうち侵入パケットの生成及び送信に関与したパケットを特定する解析手法である。ホスト内部解析の具体的手順についても後述する。

【００３０】図１の侵入経路解析装置１２４は以下の解析の開始および終了の条件に従って侵入経路解析を継続もしくは終了する。ネットワークを流れるパケットを監視している侵入検知装置からの侵入検知通知があった場合には、まず、ホストレベル解析とルータレベル解析を平行して実行する（４０１、４０９）。また、ホストの内部状態を監視する侵入検知装置から侵入検知通知があった場合には、まず、ホスト内部解析を実行する。ホストレベル解析終了時（４０２、４０３、４０４）、そのホストレベル解析と同時に開始されたルータレベル解析（たとえば、４０１で開始されたホストレベル解析に対する４０９で開始されたルータレベル解析）が未終了かつ、ホストレベル解析の結果により、ホスト内部解析の対象となるホストが侵入経路解析装置の管理下に存在する場合に、ホストレベル解析の入力としたパケットの情報を元にホスト内部解析を開始する（４０２、４０４）。その他の場合はホスト内部解析を開始しない（４０３）。ルータレベル解析終了時（４１０、４１１、４１２）、そのルータレベル解析と同時に開始されたホストレベル解析（たとえば、４０９で開始されたルータレベル解析）が未終了または、ルータレベル解析結果で得られたパケット生成ホストの発信元Ｅｔｈｅｒアドレスをキーとしたホストのアドレスとルータレベル解析の検索キーとしたパケットの発信元アドレスが異なる場合並びに、ホスト内部解析の対象となるホストが侵入経路解析装置の管理下に存在する場合に、ルータレベル解析結果ホストが送出したと断定されるパケットの情報を元にホスト内部解析を開始する（４１１、４１２）。その他の場合はホスト内部解析を開始しない（４１０）。このとき、同時に開始されたホストレベル解析によって既に別のホストに関するホスト内部解析プロセスが実行中であった場合（４１２）には、そのホスト内部解析プロセスを終了する（４０７）。ホスト内部解析終了時（４０５、４０６、４０８）、ホスト内部解析の入力としたパケットを生成したプロセスが、ネットワークを経由した外部装置からの命令を受信していた場合には、その命令を伝達したパケットを特定し、特定したパケットを入力とするホストレベル解析およびルータレベル解析を同時に起動する（４０５、４０６）。その他の場合はホストレベル解析、ルータレベル解析ともに開始しない（４０８）。これら全ての解析処理が終了した場合に侵入経路解析の終了とみなす（４１３）。

【００３１】ここで、図４に示した例について概説する。ただし、便宜上、実行されるホストレベル解析、ルータレベル解析はいずれかのホストについてのホスト内部解析を可能であるという結果が得られるものとする。同様に、実行されるホスト内部解析結果は、４０７で終了される解析と４０８で終了する解析を除いて、ホスト内部解析の後に継続してホストレベル解析およびルータレベル解析を実行可能であるという結果が得られるものとする。ネットワークを流れるパケットを監視している侵入検知装置から侵入検知通知があり、４０１及び４０９においてホストレベル解析とルータレベル解析が同時に開始される。４０２においてホストレベル解析が完了し、ホストレベル解析の結果、侵入パケットの送信元として、侵入経路解析装置と同じネットワークに属するホストのいずれかが検出される。なお、以下では、侵入経路解析装置と同じネットワークに属するホストを内部ホストと記す。また、４０１～４０２のホストレベル解析で検出された内部ホストを内部ホストＡと称する。４０

２においてホストレベル解析が終了したときに、終了したホストレベル解析と同時に開始されたルータレベル解析が未終了であるので、引き続きホスト内部解析が行われる。ホスト内部解析では、ホストレベル解析で検出された内部ホストＡの内部プロセスについて解析が行われる。一方、４１０においてルータレベル解析が完了するが、ルータレベル解析での検出結果は、先に完了しているホストレベル解析の検出結果と同じなので、ホスト内部解析はそのまま実行される。４０５で、ホスト内部解析が完了し、内部ホストＡが受信したパケットのうち侵入パケットの生成及び送信に関与したパケット（以下、侵入パケットと記す）が特定される。４０５でホスト内部解析が完了したので、ホスト内部解析により特定された侵入パケットに対して、ホストレベル解析とルータレベル解析とが同時に開始される。４１１において、ルータレベル解析が完了し、ルータレベル解析の結果、侵入パケットの送信元として内部ホストＢが検出される。ルータレベル解析により内部ホストＢが検出されたので、内部ホストＢの内部プロセス状況についてホスト内部解析が開始される。一方、４０３で、ホストレベル解析が完了するが、既にルータレベル解析の結果によるホスト内部解析が実行されているため、ルータレベル解析の結果を優先し、４１１で実行されたホスト内部解析を継続する。４０６で、ホスト内部解析が完了し、内部ホストＢが受信したパケットのうち侵入パケットの生成及び送信に関与した侵入パケットが特定される。４０６でホスト内部解析が完了したので、ホスト内部解析により特定された侵入パケットに対して、ホストレベル解析とルータレベル解析とが同時に開始される。４０４で、ホストレベル解析が完了し、ホストレベル解析の結果、侵入パケットの送信元候補として内部ホストＣが検出される。そして、ホストレベル解析で検出された内部ホストＣの内部プロセス状況についてホスト内部解析が開始される。一方、４１２で、ルータレベル解析が完了し、ホストレベル解析で検出された内部ホストＣと異なる内部ホストＤが侵入パケットの送信元として検出される。この場合、ルータレベル解析での検出結果はホストレベル解析での検出結果よりも正確性が高いので、内部ホストＣに対して実行中であったホスト内部解析を終了し、ルータレベル解析で検出された内部ホストＤの内部プロセスについてホスト内部解析を開始する（４０７）。図４の例では、ホスト内部解析の結果、内部ホストの侵入パケット生成・侵入に関与したパケットが検出されなかったので、内部ホストＤを攻撃者の端末または攻撃者の端末が直結されたホストであると断定して全ての解析処理を終了する場合を示している（４０８、４１３）。

【００３２】次に、ルータレベル解析の処理手順について説明する。まず、ルータレベル解析の基本的な原理について説明する。侵入経路解析装置は、侵入検知装置により、ホストへの侵入パケットが検知された場合に、検知された侵入パケットのヘッダとデータ管理装置のデータベース内に格納されているヘッダ情報とを比較し、ＥｔｈｅｒアドレスおよびＴＴＬを除き侵入パケットのヘッダと同じ内容のヘッダ情報を抽出する。この抽出されたヘッダ情報は、ＥｔｈｅｒアドレスとＴＴＬ以外の情報が侵入パケットのヘッダと一致しているので、侵入パケットに関するヘッダ情報であると考えることができる。そして、抽出されたヘッダ情報について送信元Ｅｔｈｅｒアドレスおよび、宛先Ｅｔｈｅｒアドレスおよび、ＴＴＬの更新経過を順次遡ることにより侵入パケットの送信元を検出する。以上が、ルータレベル解析の基本的な原理である。では、次に、図５、図６並びに、図７を参照しながら、ルータレベル解析について具体的に説明する。

【００３３】図５において、５０１から５０５はホスト、５０６から５０８はルータ、５０９から５１２は各機器を結ぶネットワーク、５１３から５１６はパケット収集装置、５１７は侵入検知装置、Ｍ１からＭ１１は各機器が持つＥｔｈｅｒアドレスを表している。

【００３４】図６において、６０１から６１３はそれぞれ図５のホスト５０１から５０４の計４つのホストからホスト５０５（ＥｔｈｅｒアドレスはＭ１１）へパケットのヘッダが全く等しい（Ｅｔｈｅｒアドレス及びＴＴＬを除く）攻撃パケットを送信したとき、図５の侵入検知装置５１７が検知するパケット６０８、６０９、６１２、６１３の何れかを検索キーとしてデータベース検索を行って得られた検索結果を表す。ただし、図６では、得られた検索結果をヘッダ情報のＴＴＬ値によって分類して記載してある。ヘッダ情報は便宜上、発信元Ｅｔｈｅｒアドレスおよび、宛先Ｅｔｈｅｒアドレスおよび、ＴＴＬ値と、それら以外の情報（パケットの検索に用いた、ＩＣＭＰプロトコルヘッダのＴｙｐｅ、Ｃｏｄｅ、Ｃｈｅｃｋｓｕｍ、ＩＰプロトコルヘッダのＩｄｅｎｔｉｆｉｃａｔｉｏｎ、Ｐｒｏｔｏｃｏｌ、発信元ＩＰアドレス、宛先ＩＰアドレス、ＴＣＰ／ＵＤＰプロトコルヘッダの発信元ポート番号、宛先ポート番号、ＣｈｅｃｋｓｕｍおよびＴＣＰプロトコルヘッダのＳｅｑｕｅｎｃｅＮｕｍｂｅｒ、ＡｃｋｎｏｗｌｅｄｇｍｅｎｔＮｕｍｂｅｒなどが含まれ、図６ではＸで表記）の４つに区別して表される。図７において、７０１は図６のパケット６０９を検索キーとしてルータレベル解析を行った侵入経路解析結果、７０２は図６のパケット６１２（またはパケット６１３）を検索キーとしてルータレベル解析を行った侵入経路解析結果を表している。

【００３５】ここでは、図６のパケット６０９のルータレベル解析を行うものとする。パケット６０９を検索キーとしてデータベース検索を行った結果をＩＰプロトコルのＴＴＬ値によって分類すると図６のような分類が得られる。

【００３６】次に、データベース検索により得られた結果に含まれるヘッダ情報のうち、パケット６０９のＴＴ

Ｌ値より小さいＴＴＬ値を持つヘッダ情報を破棄する。これは、攻撃パケット送信ホストから攻撃を受けたホスト５０５までの経路上では、パケットの宛先ＩＰアドレスが受信したパケットのＴＴＬ値が最小となることによる。したがって、ＴＴＬ値として７を持つパケット６１２とパケット６１３は、ここでデータベース検索結果から破棄される。

【００３７】ＴＴＬ値がパケット６０９と同じ、８のものがデータベース検索により得られた結果に存在する場合には、ＴＴＬ値が８に分類されるヘッダ情報から、パケット６０９と発信元Ｅｔｈｅｒアドレス並びに、宛先Ｅｔｈｅｒアドレスが等しいヘッダ情報以外のヘッダ情報を破棄する。したがって、パケット６１０とパケット６１１は、ここでデータベース検索結果から破棄される。

【００３８】次にＴＴＬ値が９のヘッダ情報について処理を行う。まず、ＴＴＬ値が８を持つパケットで残っているヘッダ情報（パケット６０９）の発信元Ｅｔｈｅｒアドレスを持つルータ５０８が持つ全てのＥｔｈｅｒアドレスを調べる。このとき、ルータ５０８はＭ１０とＭ９をＥｔｈｅｒアドレスとして持つことがわかる。次に、ＴＴＬ値が９に分類されるヘッダ情報のうち、Ｍ１０またはＭ９を宛先Ｅｔｈｅｒアドレスとして持つパケット６０７を選択し、残りを破棄する。したがって、パケット６０５、パケット６０６、パケット６０８は、ここでデータベース検索結果から破棄される。

【００３９】同様に、ＴＴＬ値に９を持つパケットで残っているヘッダ情報（パケット６０７）の発信元ＥｔｈｅｒアドレスＭ８をＥｔｈｅｒアドレスとして持つルータ５０７が持つ全てのＥｔｈｅｒアドレスを調べる。このとき、ルータ５０７はＭ８とＭ７をＥｔｈｅｒアドレスとして持つことがわかる。次に、ＴＴＬ値が１０に分類されるヘッダ情報のうち、Ｍ８またはＭ７を宛先Ｅｔｈｅｒアドレスとして持つパケット６０３を選択し、残りを破棄する。したがって、パケット６０１、パケット６０２、パケット６０４は、ここでデータベース検索結果から破棄される。

【００４０】ＴＴＬ値に１０を持つパケットで残っているヘッダ情報（パケット６０３）の発信元ＥｔｈｅｒアドレスＭ３をＥｔｈｅｒアドレスとして持つルータが持つ全てのＥｔｈｅｒアドレスを調べる。しかしながら、Ｍ３はルータが持つＥｔｈｅｒアドレスではないため、Ｍ３をＥｔｈｅｒアドレスとして持つルータは検出されない。ここで、パケット６０３は、ＥｔｈｅｒアドレスＭ３を持つホスト５０３から発信されたと断定する。したがって、パケット６０９は、ホスト５０３から発信されルータ５０７およびルータ５０８によって中継されホスト５０５へ到達したという、図７の７０１の結果が得られる。

【００４１】図６のパケット６１２（もしくはパケット６１３）に関して上記の処理を行った場合は、図５のホスト５０１とホスト５０２がともにパケットの発信ホストとして特定され、図７の７０２のような結果が得られる。

【００４２】以上のように、ルータレベル解析は、パケットのＩＰアドレスによらず解析を行うので、ＩＰアドレスを詐称された場合でも正確に侵入パケットの送出ホストと中継経路を特定できる反面、一般的には解析に時間がかかる。

【００４３】ここでは、図８を参照しながら侵入パケットの情報を初期入力とするホスト内部解析の説明を行う。図８において、８１０はホスト（踏み台）、８０１から８０７はホスト８１０上で起動されたプロセス、８１１、８１２は外部装置、８０８は外部装置８１１との通信並びに、８０９は外部装置８１２との通信に使用されたホスト８１０上の通信ポートを表している。なお、外部装置とは、他のホストまたはルータを意味する。プロセス８０１からプロセス８０７の間には、他のプロセスによって起動された側と起動した側という、いわゆるプロセスの親子関係が成り立っている。たとえば、図８において、プロセス８０５、プロセス８０６は、プロセス８０４によって起動されている。この場合、プロセス８０５およびプロセス８０６をプロセス８０４の子プロセス、プロセス８０４をプロセス８０５、プロセス８０６親プロセスと呼ぶ。ここでは、ホスト８１０は外部装置８１１から外部装置８１２へ攻撃を行う際の踏み台ホストとして使用されたものとする。

【００４４】侵入経路を外部装置８１２の側から前述のホストレベル解析もしくは、ルータレベル解析が既に行われており、解析の結果、パケットはホスト８１０の通信ポート８０９から送信されたことが特定されているものとする。このとき、そのパケット取得日時を検索キーとしてデータベースを検索し、その時間にホスト８１０の通信ポート８０９を使用していたプロセス（パケット生成プロセス）に関する情報（プロセス生成日時、プロセス終了日時、プロセス識別子、親プロセス識別子、実ユーザ識別子、実行ユーザ識別子、実グループ識別子、実行グループ識別子、実行ディレクトリ、実行コマンドパス、実行コマンドライン、通信開始日時、通信終了日時、通信先ＩＰアドレス、通信先ＴＣＰ／ＵＤＰポート番号、通信ＮＩＣに割り当てられていたＥｔｈｅｒアドレスとＩＰアドレス、ＴＣＰ／ＵＤＰポート番号）を得る。このとき、パケット生成プロセスが外部装置からの接続による通信を確立していた場合（パケット受信プロセスが行われていた場合）は、通信開始日時、通信終了日時、通信先ＩＰアドレス、通信先ＴＣＰ／ＵＤＰポート番号、通信ＮＩＣに割り当てられていたＥｔｈｅｒアドレスとＩＰアドレス、ＴＣＰ／ＵＤＰポート番号を検索キーとして、データベースを検索し、外部装置から受け取ったパケットを特定する。この特定したパケット

は、ホスト８１０の攻撃パケットの生成に関与したパケットである。そして、この特定したパケットについて、ルータレベル解析及びホストレベル解析を行い、このパケットの送信元を特定する。パケット生成プロセスが外部装置からの接続による通信を確立していなかった場合は、同様の処理を親プロセスに対して行う。

【００４５】パケット生成プロセスが外部装置からの接続による通信を確立していたプロセスが見つかるか、親プロセスが定義されないプロセス（オペレーティングシステムの特別なプロセス）にたどり着くまで、上記の処理を繰り返し行う。親プロセスが定義されないプロセスにたどりついた場合には、そのホストを、攻撃者が直接利用したコンピュータであると断定する。

【００４６】図８の例では、プロセス８０３が外部装置からの接続による通信を確立していたプロセスとなるため、プロセス８０３に関する情報を検索キーとしてデータベースを検索し、プロセス８０３が外部装置から受け取ったパケットを特定する。

【００４７】ホスト内部のプロセス情報を初期入力とするホスト内部解析（ホスト内部を監視する侵入検知装置により解析対象となるホストが特定された場合）では、上記のパケットの情報を初期入力とするホスト内部解析のホスト上でパケットを生成したプロセスに関する情報を得る処理から解析を開始し、後の処理は、パケットの情報を初期入力とする処理と同様である。

【００４８】以上のように、ホストレベル解析、ルータレベル解析並びに、ホスト内部解析を並行して行うことから、解析結果の正確性を保証しつつ、高速に侵入経路解析を行うことができる。また、ヘッダ情報並びに、ホスト内部情報をデータ管理装置でデータベースにより集中管理するため、ホストレベル解析、ルータレベル解析並びに、ホスト内部解析を行う際に、侵入経路解析中は各装置間で通信を行いながら、経路上の各ルータを逐次追跡する必要がないことからも侵入経路解析時間の短縮効果がある。

【００４９】実施の形態２．以上の実施の形態１では、過去における侵入に関しても追跡可能とするために、ネットワーク上を流れるパケットおよびホスト上のプロセスの情報を常時取得し、記録していた。この場合、記録したデータを保存するために、大容量の記憶領域を消費する。しかしながら、導入するシステムの環境によっては、データを保持しておくための大容量記憶領域の確保が難しい場合もあるため、以下のような方法により適宜情報を圧縮することもできる。第一に、記録する各パケットのデータのうち、侵入経路解析で用いる項目（パケット取得日時並びに、パケットを識別するために一般的に用いられるパケットヘッダ内の発信元ＥｔｈｅｒアドレスⅠ、宛先ＥｔｈｅｒアドレスⅠ、ＩＣＭＰプロトコルヘッダのＴｙｐｅⅠ、ＣｏｄｅⅠ、ＣｈｅｃｋｓｕｍⅠ、ＩＰプロトコルヘッダのＩｄｅｎｔｉｆｉｃａｔｉｏｎⅠ、ＴＴＬⅠ、ＰｒｏｔｏｃｏｌⅠ、発信元ＩＰアドレスⅠ、宛先ＩＰアドレスⅠ、ＴＣＰ／ＵＤＰプロトコルヘッダの発信元ポート番号、宛先ポート番号、ＣｈｅｃｋｓｕｍⅠ、ＴＣＰプロトコルヘッダのＳｅｑｕｅｎｃｅＮｕｍｂｅｒⅠ、ＡｃｋｎｏｗｌｅｄｇｍｅｎｔＮｕｍｂｅｒⅠ）だけを記録していく。第二に、侵入経路解析装置より侵入経路データ提出要求があったときのみ各パケット取得装置並びに、各ホスト内部情報収集装置で同時に情報収集を開始する。どちらの場合も、解析するシステムの大きさにより、データを保持する期間を決めて一定期間を過ぎたデータから随時削除していくことも可能である。

【００５０】以上のように、常時保持するデータの量を制限することで、侵入経路解析に使用される記憶領域容量を軽減できる。ただし、データを保持しておく期間は、適用するシステムの性能並びに、要求される解析結果の詳細度によって決定される。

【００５１】実施の形態３．以上の実施の形態１並びに実施の形態２では、少なくとも解析を行う段階においてデータベースに検索対象となるデータが格納されていれば侵入経路解析には影響を及ぼさない。したがって、各パケット取得装置並びに、各ホスト内部情報収集装置で収集したデータを常時データベース管理装置に格納する必要はなく、侵入経路解析を行わないときには、各パケット収集装置並びに、各ホスト内部情報収集装置で収集したデータを保持しておき、侵入経路解析を行う際に各装置から一斉に記録データ（パケットの情報並びに、ホスト上のプロセス情報）をデータ管理装置へ送信しデータベースへ格納することもできる。

【００５２】以上の実施の形態３によれば、収集データの分散管理が可能であり、侵入経路解析未実行時のデータ管理装置上のリソースに対する負荷（記憶領域容量並びにデータ処理など）を削減できる。

【００５３】実施の形態４．以上の実施の形態３では、侵入経路解析を行う際に各装置から一斉に記録データ（パケットの情報並びに、ホスト上のプロセス情報）をデータ管理装置へ送信しデータベースへ格納することで、侵入経路解析未実行時の収集データの分散管理を行った。これに加え、各パケット収集装置上にルータレベル解析機能並びに、各ホスト内部情報収集装置上にホスト内部解析機能を備え、侵入経路解析装置が侵入経路解析のスケジューリング並びに、ホストレベル解析を行うようにした場合には、侵入経路解析時に侵入経路解析装置にかかる計算負荷を軽減できる。

【００５４】以上の実施の形態４によれば、ネットワーク上に分散している各パケット収集装置並びに、各ホスト内部情報収集装置上へ侵入経路解析処理を分散しているため、侵入経路解析時に侵入経路解析装置にかかる計算負荷を軽減できる。加えて、実装上パケット収集装置並びに、ホスト内部情報収集装置がそれぞれルータ並びにホスト上に実装されていた場合、当該不正アクセス処

理が継続中である場合には、ルータやホストのその他の処理を意図的に遅延されることも可能であり、不正アクセス処理を遅延する効果もある。

【００５５】実施の形態５．以上の実施の形態１～４では、単一の侵入経路解析装置を用いた場合の実施の例であったため、侵入経路解析の範囲に限界がある。そこで、実施の形態５では、複数の侵入経路解析装置を用いて、より広範囲な侵入経路解析を行う方式について説明する。

【００５６】図９において、９０１、９０２、９０３はそれぞれ異なる侵入経路解析装置、９０４、９０５、９０６はそれぞれ侵入経路解析装置９０１、９０２、９０３が経路解析可能なネットワーク、９０７～９１０は侵入経路上のホストを表している。なお、各ネットワークとも、図１に示したように、侵入検知装置、パケット収集装置等が配置されているものとする。各ホスト間を結ぶ直線上にはパケットを中継する複数のルータが存在している。図９では、ホスト９０７を攻撃者端末とし、攻撃者はホスト９０８およびホスト９０９を踏み台としてホスト９１０を攻撃したものとする。

【００５７】侵入経路解析装置９０３は、前述の方法で侵入経路解析を行った結果、ホスト９１０への不正アクセスパケットは、侵入経路解析装置９０２によって追跡可能なネットワーク上の装置（ホストまたはルータ）から送信されたパケットであると断定する。このとき、侵入経路解析装置９０３は、ネットワーク９０５からネットワーク９０６へ送られてきたパケットの情報を含む検出依頼を侵入経路解析装置９０２に送信し、侵入経路解析の継続を依頼する。

【００５８】検出依頼を受領した侵入経路解析装置９０２は、侵入経路解析装置９０３から送られてきたパケット情報を元に、実施の形態１～４に示す方式に従って侵入経路解析を行う。このとき、ネットワーク９０５上のホスト９０８およびホスト９０９が踏み台とされたこと、並びに、ホスト９０８は侵入経路解析装置９０１が解析可能なネットワーク上の装置（ホストまたはルータ）から送信されたパケットであると断定する。侵入経路解析結果を侵入経路解析装置９０３に送信する。

【００５９】侵入経路解析装置９０３は、侵入経路解析装置９０２の解析結果に含まれる、侵入経路解析装置９０２からのパケット情報を含む検出依頼を侵入経路解析装置９０１へ送信し、侵入経路解析の継続を依頼する。

【００６０】侵入経路解析装置９０１でも、侵入経路解析装置９０２と同様に侵入経路解析を行い、検出依頼のあったパケットは、ホスト９０７から発信されたことを特定し、解析結果を侵入経路解析装置９０３に送信する。

【００６１】最終的に、侵入経路解析装置９０３は、ネットワーク９０６の解析結果、並びに、侵入経路解析装置９０２、侵入経路解析装置９０１から送信されてきた結果から、ホスト９０７からホスト９１０までの一連の侵入経路を特定する。

【００６２】以上の実施の形態５によれば、複数の侵入経路解析装置が連携し、個々のネットワーク内の解析結果を統合しているため、複数のネットワークにわたるような広範囲な侵入経路解析ができる。

【００６３】以上の実施の形態１～５では、本発明に係る不正アクセス経路解析システム（侵入経路解析システム）について説明したが、実施の形態１～５に示した処理手順により本発明に係る不正アクセス経路解析方法も実現可能である。

【００６４】ここで、実施の形態１～５に示した侵入経路解析システムの特徴を以下にて再言する。

【００６５】実施の形態１～５に示す侵入経路解析システムは、以下の装置を有することを特徴とする。

１．外部装置からの命令を受信もしくは、自動もしくは、手動で起動し、ネットワーク上を流れるパケットを収集し、記録し、外部装置による記録データ送信要求発行時もしくは、定期的に外部装置へ記録データを送信するパケット収集装置（複数可能）。

２．外部装置からの命令を受信もしくは、自動もしくは、手動で起動し、オペレーティングシステムによって管理されるホスト上のプロセス管理情報並びに、そのプロセスのプロセス間通信履歴に関する情報（これらを総称してホスト内部情報と呼ぶことがある）を収集し、記録し、外部装置による記録データ送信要求発行時もしくは、定期的に外部装置へ記録データを送信するホスト内部情報収集装置（複数可能）。

３．ネットワーク上に存在するパケット収集装置並びに、ホスト内部情報収集装置へ記録データ送信要求発行後もしくは、定期的にパケット収集装置並びにホスト内部情報収集装置から送信される記録データを受信し、データベースに格納するデータ管理装置（複数可能）。

４．外部装置からの命令を受信もしくは、自動もしくは、手動で起動し、ホストレベル解析機能、ルータレベル解析機能、ホスト内部解析機能を持ち、それぞれの解析を平行して実行可能である侵入経路解析装置（複数可能）。

５．ネットワーク上を流れるパケットを監視もしくはホストの内部状態を監視することで侵入を検知し、検知した情報を外部装置へ通知する侵入検知装置。

【００６６】実施の形態１～５に示す侵入経路解析システムは、ヘッダ情報を検索キーとしてデータベース検索し、得られた複数の検索結果をパケット情報に含まれるＴＴＬ（Ｔｉｍｅ　ｔｏ　Ｌｉｖｅ）データ、送信元ＥｔｈｅｒアドレスまたはＥｔｈｅｒアドレスを用いて解析することを特徴とする。

【００６７】実施の形態１～５に示す侵入経路解析システムは、ルータレベル解析と、ホスト内部情報を用いたホスト内部解析とを行うことを特徴とする。

【００６８】実施の形態１～５に示す侵入経路解析システムは、ルータレベル解析並びに、パケット情報に含まれる発信元ＩＰアドレスによるパケットの発信元解析を行うホストレベル解析並びに、ホスト内部解析を併用して侵入経路解析を高速化することを特徴とする。

【００６９】

【発明の効果】以上のように、本発明によれば、送信元検出処理及び内部プロセス解析処理を行うため、踏み台を介した不正アクセス、発信元アドレスを詐称した不正アクセスにも対応可能であり、解析結果の正確性を保証しつつ、高速に不正アクセス経路解析を行うことができる。

【００７０】また、本発明によれば、第一の送信元検出処理と第二の送信元検出処理とを並行して行うため、第一の送信元検出処理により解析結果の正確性を保証することができ、また、第二の送信元検出処理により解析処理の高速化を図ることができる。

【００７１】また、本発明によれば、パケットの収集及び内部プロセス情報の収集は、指示があった場合のみ行うため、ヘッダ情報及び内部プロセス情報の記憶のための記憶領域容量を軽減することができる。

【００７２】また、本発明によれば、ヘッダ情報及び内部プロセス情報は、指示があった場合のみ送信することとしているため、不正アクセス経路解析を行わないときのシステムリソースに対する負荷を削減することができる。

【００７３】また、本発明によれば、複数のネットワークに跨って不正アクセス経路解析を行うことができるため、広範囲に渡った不正アクセスの場合でも、正確かつ高速に不正アクセス経路解析を行うことができる。

【図面の簡単な説明】

【図１】　侵入経路解析システムのシステム構成例を示す図。

【図２】　従来の技術を説明する図。

【図３】　従来の技術を説明する図。

【図４】　侵入経路解析スケジューリング例を示す図。

【図５】　ルータレベル解析例を説明するためのシステム構成図。

【図６】　ヘッダ情報の例を示す図。

【図７】　ルータレベル解析の結果の例を示す図。

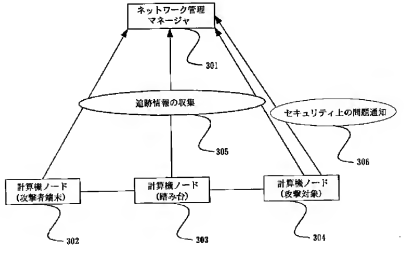
【図８】　ホスト内部解析例を説明するためのプロセス経過図。

【図９】　複数の侵入経路解析システムを用いた解析例を説明するためのシステム構成図。

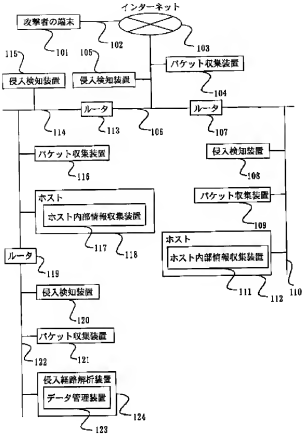
【符号の説明】

１０１　攻撃者の端末、１０２　経路、１０３　インターネット、１０４　パケット収集装置、１０５　侵入検知装置、１０６　サブネットワーク、１０７ルータ、１０８　侵入検知装置、１０９　パケット収集装置、１１０　サブネットワーク、１１１　ホスト内部情報収集装置、１１２　ホスト、１１３　ルータ、１１４　サブネットワーク、１１５　侵入検知装置、１１６　パケット収集装置、１１７　ホスト内部情報収集装置、１１８　ホスト、１１９　ルータ、１２０　侵入検知装置、１２１　パケット収集装置、１２２　サブネットワーク、１２３　データ管理装置、１２４　侵入経路解析装置。

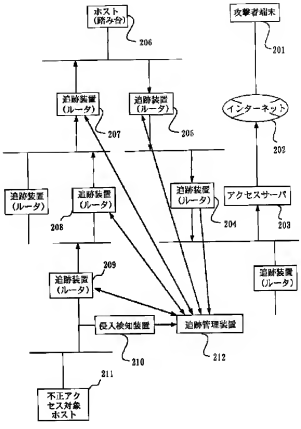
【図３】



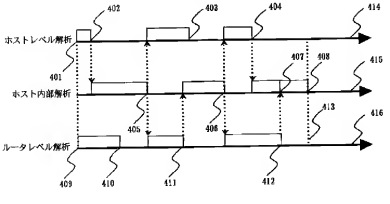
【図１】


インターネット
攻撃者の端末
101
102
103
115
105
侵入検知装置
侵入検知装置
パケット収集装置
104
ルータ
ルータ
114
113
106
107
パケット収集装置
116
侵入検知装置
108
ホスト
ホスト内部情報収集装置
パケット収集装置
109
117
118
ホスト
ホスト内部情報収集装置
ルータ
119
111
112
110
侵入検知装置
120
パケット収集装置
122
121
侵入経路解析装置
データ管理装置
124
123

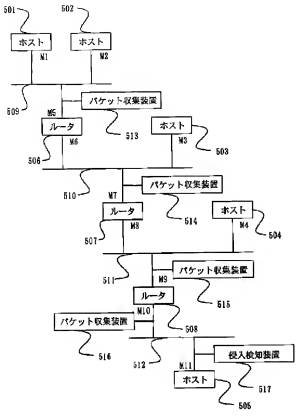
【図２】


ホスト
(踏み台)
206
攻撃者端末
201
追跡装置
(ルータ)
207
追跡装置
(ルータ)
205
インターネット
202
追跡装置
(ルータ)
208
追跡装置
(ルータ)
追跡装置
(ルータ)
204
アクセスサーバ
203
209
追跡装置
(ルータ)
追跡装置
(ルータ)
侵入検知装置
追跡管理装置
210
212
211
不正アク
セス対象
ホスト

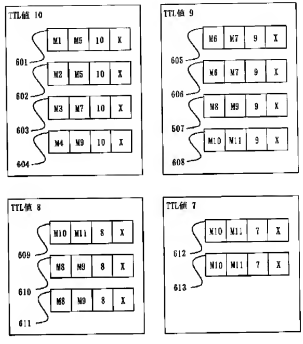
【図４】


ホストレベル解析
ホスト内部解析
ルータレベル解析
401
402
403
404
414
407
408
415
405
406
413
416
409
410
411
412

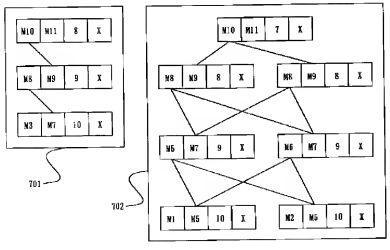
【図５】


501
502
ホスト
ホスト
M1
M2
509
M5
パケット収集装置
ルータ
513
ホスト
M6
M3
503
506
510
M7
パケット収集装置
ルータ
514
ホスト
M8
M4
504
507
511
M9
パケット収集装置
ルータ
515
M10
パケット収集装置
508
516
512
M11
侵入検知装置
ホスト
517
505

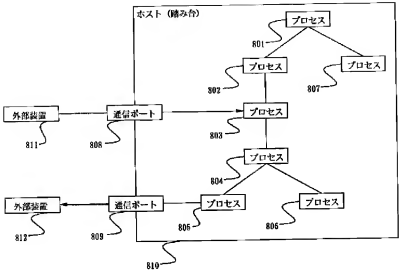
【図６】


TTL値 10
M1 M5 10 X
601
M2 M5 10 X
602
M3 M7 10 X
603
M4 M9 10 X
604
TTL値 9
M6 M7 9 X
605
M8 M7 9 X
606
M8 M9 9 X
607
M10 M11 9 X
608
TTL値 8
M10 M11 8 X
609
M8 M9 8 X
610
M8 M9 8 X
611
TTL値 7
M10 M11 7 X
612
M10 M11 7 X
613

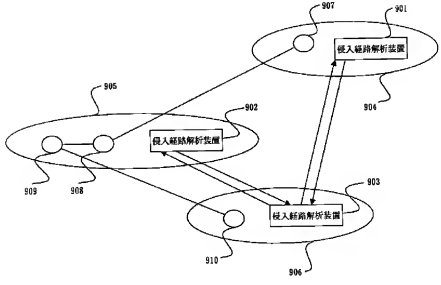
【図７】


M10 M11 8 X
M8 M9 9 X
M3 M7 10 X
701
M10 M11 7 X
M8 M9 8 X
M8 M9 8 X
M5 M7 9 X
M6 M7 9 X
M1 M5 10 X
M2 M6 10 X
702

【図８】


ホスト（踏み台）
プロセス
801
プロセス
プロセス
802
807
外部装置
通信ポート
プロセス
811
808
803
プロセス
804
外部装置
通信ポート
プロセス
プロセス
812
809
805
806
810

【図９】


907
901
侵入経路解析装置
905
904
902
侵入経路解析装置
909
908
903
侵入経路解析装置
910
906